IT Unit 4

Topic 2

**Ch 6, Security Measures** (Informatics, p 280-280)

**Disaster recovery plans**

1. What is a disaster recovery plan?

A disaster recovery plan is a comprehensive scheme that explains how to prepare for, survive and recover from a disaster that affects information systems infrastructure.

1. What are the benefits of a DRP?

It provides a sense of security and confidence to workers, it prevents a sense of security and confidence to workers, it prevents further problems that might be caused by panic, it reduces the amount of uncertainty and decision-making in stressful moments and it neatly explains procedures to new employees.

1. List the four main components of a DRP.

Evacuation, backing up data, data restoration and testing of disaster plans.

1. A Creating a DRP:
   1. Scope
      1. What does a risk assessment involve?

Risk assessment analyses the probability of different risks to your data and information, and the potential consequences of each of those risks.

* + 1. What is a contingency plan?

A contingency plan is a backup plan if the preferred procedure happens to be unavailable.

* + 1. Why is it important to allocate emergency responsibilities?

It is important to allocate emergency responsibilities to state clearly who is responsible for doing what, where and when.

* + 1. What does an audit involve?

An audit is an official inspection of all digital systems which includes make, model and version numbers.

* + 1. How should key information be kept?

Document key information should be kept in printed dorm so it can be easily found during an emergency evacuation.

**Backup scheme**

1. Distinguish between the following backup schemes:
   1. Daily incremental

A backup of new or changed data since the last full or incremental backup that is quick and consumes less storage space than a full backup. Many media

* 1. Weekly full

A backup of all files in the entire system, including the operating system

* 1. Differential

Similar to an incremental backup, but saves changes since the last full backup. Two media

* 1. Partial

Only backs up a portion of the file system, such as a folder or individual files within a file system, such as a single hard disk or multiple-disk array.

1. What is meant by continuous data protection and why is it becoming popular?

Continuous data protection saves all versions of all data immediately when it is created or change, and saves it offside using the cloud or a remote network server.

**Backup media**

1. List the strengths and weaknesses of the following backup media:
   1. Tape

Strengths is that it is common and popular in the business world.

Weaknesses includes it wearing out and degrading over time, it has limited capacity, it is slow to save/restore data, they can be expensive and they’re declining in favour of network or cloud backups.

* 1. External hard drive

Strengths include it being fast, high-capacity, cheap, portable, easily available and easy to use, it can be automated and the data never leaves your control.

Weaknesses includes that they fail over time, they can be damaged by mishandling and they can be erased by a strong magnetic field.

* 1. Online, cloud

Strengths include backups occur automatically, immediately and continuously, it is relatively cheap, has offsite storage, large capacities are available and every version of a document over time can be recovered.

Disadvantages include slow to upload large files; valuable data is entrusted to an outsider and it will not work without an internet connection.

* 1. CD/DVD

Strengths include it being relatively cheap to implement, the read-only data cannot be changed later and it is very portable.

Weaknesses include it being easily damaged and it degrades over time, it has a limited capacity, must be written manually and read-only disks are not reusable.

* 1. USB flash drive

Strengths include it being small, very portable and cheap and they’re easily available and convenient.

Weaknesses include there being a limited rewrite capacity that can fail without warning, USB 2.0 devices can be slow and they can be easy to lose.

1. Where should backup media be stored?

Backup media should be stored offsite.

1. What is a NAS device?

A NAS device is a network-attached storage device.

**Testing the backup scheme**

1. Why is testing of the backup scheme vital?

Testing of the backup scheme is vital as it must be ensured that the backups will be successful. This is because if the backup is unsuccessful it be catastrophic when the day comes that you actually need to use it.

1. Outline some methods of testing a backup scheme.

Create a few typical [dummy] documents and delete them a few days later: it is important to ensure that the information is recoverable

Recover a backup of a database, video or spreadsheet that is several years’ old: it is important to check this as while most major applications try to retain their ability to open documents created in previous versions, there often comes a time when backward compatibility cannot be maintained and old documents can only be opened by old applications.

Perform integrity tests of tapes or hard disks: this will detect media faults that could lead to corrupt data

Completely restore from backup to another location or to a different hardware: this is because in a real disaster, the original hardware may need to be replaced with newer or different equipment.

Conduct failover and failback tests: this is because some advanced systems will have built-in redundancy, where all data is mirrored. If the primary system fails, the secondary equipment activates.

**Testing the disaster plan**

1. Why should DRP’s be regularly tested? What does this involve?

DRP’s should be regularly tested to ensure that the procedures remain appropriate. It involves practicing drills including evacuation drills, practice using firefighting equipment, practice shutting down systems safely and practice notifying emergency services.

1. With the recovery strategy how is the recovery verified?

Complete recovery is verified according to pre-planned criteria.

**Consequences of security failure**

1. List the potential consequences of security failure.

Loss of customer loyalty, penalties and prosecution, loss of trade secrets to competitors, decline in stock market value, loss of productivity, inability to pay staff and suppliers, loss of income and costs, labour and disruptions to recreate data and repair or replace equipment.